UNIVERSITÄT DES SAARLANDES
Fachrichtung 6.1 - Mathematik
Christian Bopp

Übungen zur Elementaren Zahlentheorie

Sommersemester 2018

Die Lösungen des Übungsblattes sind bis spätestens 14.00 Uhr, am 04.07.2018, in die Briefkästen vor dem Zeichensaal in Geb. E2 5, einzuwerfen.
Alle Übungsblätter und Informationen zur Vorlesung werden auf der Seite unserer Arbeitsgruppe unter *Teaching* zu finden sein: www.math.uni-sb.de/ag-schreyer/

Blatt 12 — 27.05.2018

Aufgabe 1.

(a) Zeigen Sie, dass 2 eine Primitivwurzel modulo 19 ist.
(b) Zeigen Sie, dass 2 keine Primitivwurzel modulo 23 ist.
(c) Ist 10 eine Primitivwurzel modulo 11?
(d) Finden Sie alle Primitivwurzeln modulo 11.

Aufgabe 2.

(a) Wiederholen Sie das RSA-Verschlüsselungsverfahren.
(b) Wir wählen 2 als Blocklänge für das RSA-Verfahren (dies macht in der Praxis natürlich wenig Sinn). Alice verschlüsselt eine Nachricht mit dem öffentlichen Schlüssel $(23, 143)$. Der Verschlüsselte Text lautet $''02''$. Bob's privater Schlüssel ist $(47, 143)$. Weisen Sie zunächst nach, dass es sich bei $(23, 143)$ (bzw. $(47, 143)$) um einen gültigen öffentlichen (bzw. privaten) Schlüssel für das RSA-Verfahren handelt (es ist $143 = 11 \cdot 13$). Wie lautet die unverschlüsselte Nachricht?

Bitte wenden.

Der Polynomring:

Sei K ein Körper (z.B. $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ oder $K = \mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p) und sei

$$K[x] = \Big\{ f(x) = \sum_{i=0}^{\infty} a_i x^i \;\Big|\; a_i \in K \text{ und } a_i = 0_K \text{ für alle bis auf endlich viele } i \in \mathbb{N} \Big\}$$

die Menge aller Polynome mit Koeffizienten in dem Körper K. Die Menge $K[x]$ ist bezüglich der Verknüpfungen

$$f(x) + g(x) = \sum_{k=0}^{\infty} (a_k + b_k) x^k$$

und

$$f(x) \cdot g(x) = \sum_{k=0}^{\infty} c_k x^k, \text{ mit } c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

(wobei $f(x) = \sum_{i=0}^{\infty} a_i x^i$ und $g = \sum_{i=0}^{\infty} b_i x^i$) ein kommutativer Ring mit Einselement (vgl. Blatt 4 Aufgabe 4).

Im folgenden definieren wir einige wichtige Begriffe zum Thema Polynomring.
Sei $f(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$. Das *Nullpolynom* $f(x) = 0$ ist das Polynom dessen Koeffizienten alle gleich Null sind. Ist $f(x) \neq 0$, so heißt die kleinste Zahl $n \in \mathbb{N}$, sodass alle $a_m = 0$ sind für $m > n$, der Grad von $f(x)$ (geschrieben $\mathrm{Grad}(f(x))$). Es ist Konvention den Grad des Nullpolynoms als $-\infty$ zu definieren. Sind $0 \neq f(x), g(x) \in K[x]$ so ist

$$\mathrm{Grad}(f(x) \cdot g(x)) = \mathrm{Grad}(f(x)) + \mathrm{Grad}(g(x)) \text{ und}$$
$$\mathrm{Grad}(f(x) + g(x)) \leq \max\{\mathrm{Grad}(f(x)), \mathrm{Grad}(g(x))\}$$

Ist $f(x) = \sum_{i=0}^{n} a_i x^i$, ein Polynom vom Grad n, so heißt $a_n x^n$ der *führende Term* von $f(x)$. Der Koeffizient a_n heißt der *Leitkoeffizient* von $f(x)$ und falls $a_n = 1$ ist, heißt das Polynom $f(x)$ *normiert*.
Sind $f(x), g(x) \in K[x]$, so sagen wir, dass $g(x)$ ein *Teiler* von $f(x)$ ist, falls ein $h(x) \in K[x]$ existiert mit $f(x) = g(x) \cdot h(x)$. Wir schreiben hierfür $g(x) \big| f(x)$.
In vielerlei Hinsicht verhält sich der Polynomring $K[x]$ wie der Ring $\mathbb{Z}$. So haben beispielsweise auch zwei Polynome einen größten gemeinsamen Teiler: Der *größte gemeinsame Teiler* zweier Polynome $f(x), g(x) \in K[x]$ ist das eindeutig bestimmte normierte Polynom größten Grades, welches sowohl $f(x)$ als auch $g(x)$ teilt.
Um diesen zu berechnen, verwendet man den euklidischen Algorithmus für den Polynomring. Hierfür benötigt man eine Version der 'Division mit Rest' für den Ring $K[x]$, die sogenannte Polynomdivision:

Aufgabe 3. Sei K ein Körper und seien $f(x), g(x) \in K[x]$ Polynome mit $g(x) \neq 0$. Zeigen Sie, dass eindeutige Polynome $q(x), r(x) \in K[x]$ existieren mit

$$f(x) = q(x) \cdot g(x) + r(x)$$

und $\mathrm{Grad}(r(x)) < \mathrm{Grad}(g(x))$.
Analog zu den ganzen Zahlen nennt man $q(x)$ den Quotienten und $r(x)$ den Rest nach Division von $f(x)$ durch $g(x)$.

Aufgabe 4.
(a) Sei K ein Körper und $f(x) \in K[x]$ ein Polynom. Zeigen Sie, dass ein Element $\alpha \in K$ genau dann eine Nullstelle von $f(x)$ ist, wenn ein Polynom $q(x) \in K[x]$ existiert mit $f(x) = q(x)(x - \alpha)$.
(b) Sei K ein Körper und $f(x) \in K[x]$ ein Polynom vom Grad n. Zeigen Sie, dass $f(x)$ höchstens n Nullstellen in K besitzt.